**ASSIGNMENT 1 FRONT SHEET**

|  |  |  |  |
| --- | --- | --- | --- |
| **Qualification** | **TEC Level 5 HND Diploma in Computing** | | |
| **Unit number and title** | **Unit 2: Networking** | | |
| **Submission date** |  | **Date Received 1st submission** |  |
| **Re-submission Date** |  | **Date Received 2nd submission** |  |
| **Student Name** | Cao Việt Hùng | **Student ID** | BH01502 |
| **Class** | SE07201 | **Assessor name** | Nguyễn Hạnh |
| **Student declaration**  I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice. | | | |
|  |  | **Student’s signature** |  |

**Grading grid**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| P1 | P2 | P3 | P4 | M1 | M2 | D1 |
|  |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **❒ Summative Feedback: ❒ Resubmission Feedback:** | | |
| **Grade:** | **Assessor Signature:** | **Date:** |
| **Internal Verifier’s Comments:** | | |
| **Signature & Date:** | | |

1. Introduction :
2. Content

**P1 Discuss the benefits and constraints of different network types and standards.**

* **Benefit :**

\*\*Local Area Networks (LANs):\*\*

- Increased data transfer speeds and reduced latency within the local network

- Improved resource sharing, such as printers, storage devices, and computing power

- Enhanced security and access control within the local The benefits of belonging to different types of networks and standards can be quite varied and significant. Let's explore a few key points:

environment

- Simplified administration and management of the network infrastructure

\*\*Wide Area Networks (WANs):\*\*

- Ability to connect geographically geographically locations and facilitates communication

- Access to shared resources and services hosted in the cloud or at remote sites

- Scalability to accommodate growing business needs across multiple locations

- Improved reliability and redundancy through alternative communication paths

- Potential cost savings by leveraging shared network infrastructure

\*\*Wireless Networks (Wi-Fi, Cellular):\*\*

- Increased mobility and flexibility for users to access the network from anywhere

- Reduced infrastructure costs by eliminating the need for extensive cabling

- Easier deployment and reconfiguration in dynamic environments

- Support for IoT (Internet of Things) devices and seamless connectivity

\*\*Industry-Specific Standards (e.g., Ethernet, Wi-Fi, Bluetooth):\*\*

- Interoperability and compatibility between devices from different manufacturers

- Established performance and security guidelines for reliable and consistent operation

- Broader ecosystem of compatible products and services, fostering innovation

- Simplified integration and deployment within existing technology frameworks

\*\*Internet Standards (e.g., TCP/IP, HTTP, SMTP):\*\*

- Global interconnectivity and the ability to communicate across the internet

- Access to a vast array of online resources, services, and applications

- Standardized protocols enabling seamless exchange of information

- Widespread adoption and support from a large community of users and developers

**- Restrict :**

There are also some limitations associated with belonging to different types of networks and standards that are important to consider:

Local Area Networks (LANs):

Limited geographical reach, typically confined to a specific building or campus

Potential for bottlenecks and performance issues if the network is overloaded

Dependency on the on-site infrastructure, which can be vulnerable to local disruptions

Challenges in seamlessly integrating remote users or branch offices

Wide Area Networks (WANs):

Higher overall costs due to the need for leased lines, managed services, or internet connectivity

Potential for latency and reduced performance compared to local networks

Increased complexity in troubleshooting and managing a distributed network infrastructure

Dependency on third-party service providers and potential reliability concerns

Wireless Networks (Wi-Fi, Cellular):

Potential for interference, signal obstructions, and coverage limitations in certain areas

Lower data transfer speeds and higher latency compared to wired networks

Security vulnerabilities and the need for robust encryption protocols

Potential for increased power consumption and battery drain on mobile devices

Industry-Specific Standards (e.g., Ethernet, Wi-Fi, Bluetooth):

Limited interoperability with devices or systems that do not adhere to the same standards

Potential for vendor lock-in and reduced flexibility in choosing compatible products

Ongoing maintenance and upgrade requirements to keep pace with evolving standards

Compatibility issues when integrating legacy systems or equipment

Internet Standards (e.g., TCP/IP, HTTP, SMTP):

Vulnerability to cyber threats, such as hacking, malware, and distributed denial-of-service (DDoS) attacks

Dependence on a reliable and stable internet connection, which can be affected by outages or network congestion

Potential for privacy and data security concerns, particularly when dealing with sensitive information

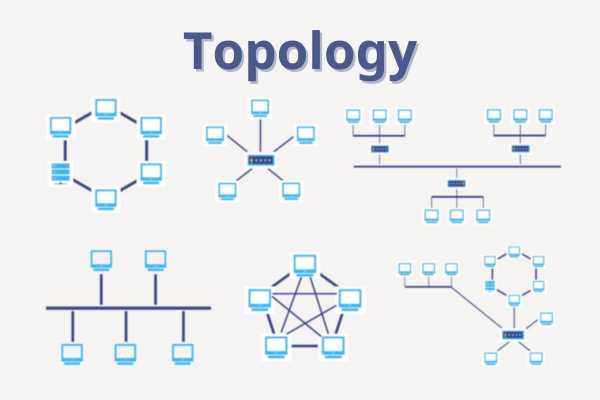
Challenges in ensuring consistent and seamless user experience across different devices and platforms

These limitations highlight the importance of carefully evaluating the trade-offs between the benefits and the potential drawbacks when choosing and implementing different types of networks and standards.

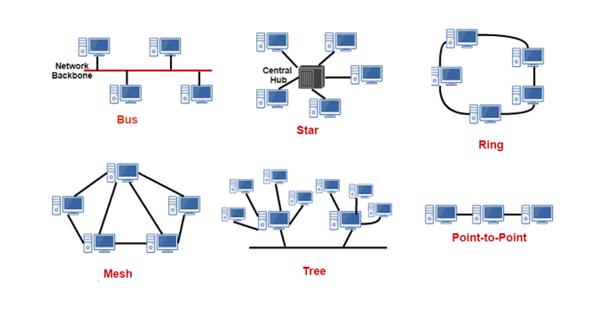
**P2 Explain the impact network topologies have on communication and bandwidth requirements.**

**1. Network Typology :**

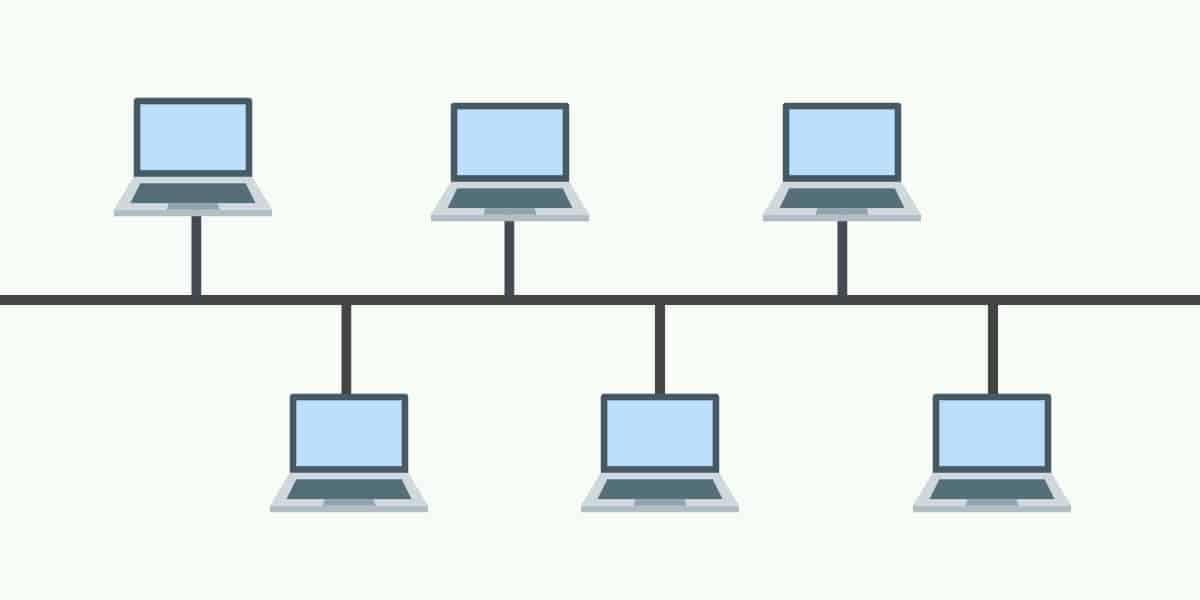
Network topology is the arrangement of the various elements (links, nodes, etc.) of a computer network.[1][2] Primarily, it is the topological structure[3] of a computer network, and can be described physically and logically. The physical topology (physical topology) is the arrangement of the various network components, including device housing and cabling installation, while the logical topology (logical topology) dictates How data flows in the network. The distance between network nodes, physical intersections, transmission rates, and/or signal patterns may vary between two networks even though their topologies may be identical

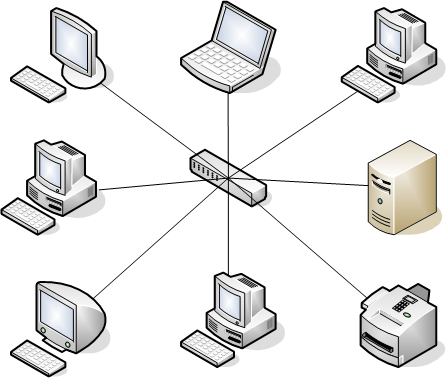
**\*** Topology (network structure) is a technical language used to describe how networks of devices are connected and organized in a computer network. It is determined how the data processing and transmission units are interconnected and arranged like anyone else in the network . 

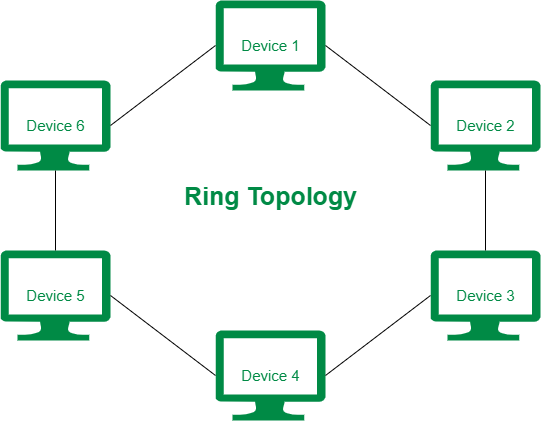
- Physical Topology:

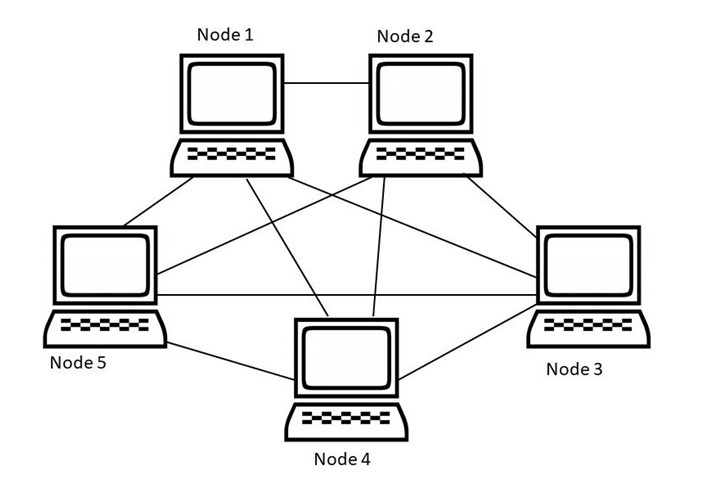


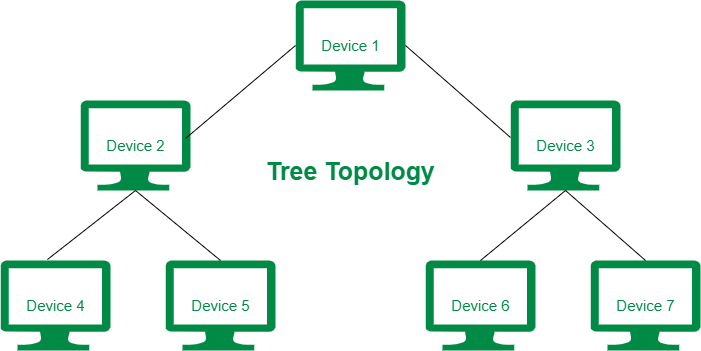
Physical topology describes how network devices (such as computers, switches, routers, etc.) are physically connected to each other through transmission media such as copper cables, fiber optic cables, or radio waves. Common types of physical topologies include:

Bus Topology (Bus network): Devices connect to a single common transmission line. Data is transmitted over this link and all devices can see it, but only the destination device receives the data. 

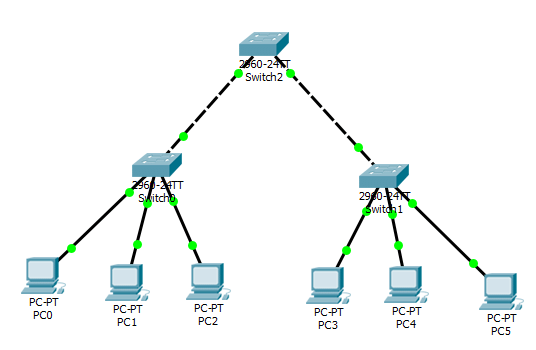
Star Topology: All devices connect to a central device, usually a switch or hub. Central device that manages and controls network traffic. 

Ring Topology: Devices connect in a closed circle. Data is transmitted in one direction around the ring, from one device to another. 

Mesh Topology: Each device in the network connects directly to all other devices. This is the most complex topology but provides high redundancy. 

Tree Topology (Tree network): Combination of star network and bus network. Devices are organized in a hierarchical structure with a root node and child nodes. 

2. Logical Topology



The logical topology describes how data moves across the network and how devices communicate with each other, regardless of how they are physically connected. Common types of logical topologies include

* Logical Bus Topology: Data is transmitted on a common logical bus, similar to a physical bus topology, but may not be the only physical bus.
* Logical Ring Topology: Data moves in a logical ring, similar to a physical ring topology, but does not necessarily have a ring-shaped physical connection.
* Logical Star Topology: Data is sent to a logical central point, similar to a physical star topology, but the central point can be a software or a server.

\* **The division by connection form of WAN and LAN networks can be expressed as follows:**

Wide Area Network (WAN - Wide Area Network)

A WAN is a network that connects smaller networks, like LANs, across large geographic areas, such as countries or the globe. Connection forms in WAN often include:

Point-to-Point:

Two network devices are directly connected to each other.

Used to connect remote offices or branches of a company to the headquarters.

For example: Connect T1, E1.

Star:

Each LAN connects to a central point, usually a central router or switch.

The central point manages and routes data between subnets.

Creates ease of management but the central point becomes a potential bottleneck.

Mesh (Mesh shape):

Each subnet in the WAN is connected to many other subnets.

Provides high redundancy and enhances network reliability.

All points can communicate with each other without going through an intermediary point.

Local Area Network (LAN - Local Area Network)

LAN is a network that connects devices in a limited area such as a building or an office. Connection forms in LAN often include:

Star:

Devices connect to a central switch or hub.

Most popular in modern LANs thanks to its high performance and ease of management.

Creates a single point of failure at the central device.

Bus (Bus image):

All devices connect to a single line (bus).

Data travels over a common link and all devices can see the data, but only the destination device receives the data.

Currently less popular due to performance issues and difficulty in scaling.

Ring:

The devices are connected in a closed circle.

Data moves in one direction around the ring.

May cause problems if a connection is broken.

Tree (Tree image):

Combination of star network and bus network.

Devices are organized in a hierarchical structure with a root node and child nodes.

Easy to scale and manage but can be complicated to configure.

Hybrid (Mixed):

Combine different connection types to take advantage of the advantages of each type.

For example, a LAN can combine a star network and a bus network.

Flexible and customizable to meet specific requirements.

Compare WAN and LAN according to connection type

Geography: WAN connects large areas, while LAN is limited to a small area.

Transmission media: WAN often uses long-distance connections such as fiber optic cable, satellite, and MPLS, while LAN often uses Ethernet cable, Wi-Fi.

Speed: LAN usually has higher speed than WAN due to shorter data transmission distance.

Cost: The cost of setting up and maintaining a WAN is often higher than a LAN due to more complex infrastructure and technology requirements.

2. **Communicate :**

+ Determine commutation in terms of network connection :

1. Circuit Switching

Commutative circuits establish a fixed path between two points before data is transmitted. This transmission line remains intact throughout the communication process.

Advantage:

High reliability, data is transmitted along a fixed path.

Ensure stable bandwidth and service quality.

Defect:

Inefficient use of resources, because the connection is held up even when there is no data to transmit.

Connection establishment time may take a long time.

For example: Traditional telephone systems use commutative circuits.

2. Packet Switching

Packet commutation divides data into small packets and each packet is transmitted independently over the network. Packets can travel through different paths and be reassembled at the destination.

Advantage:

Use network resources effectively, no need to keep a fixed connection.

Increasing reliability, if one link fails, packets can be redirected over another path.

Good support for applications that need high speed and flexibility.

Defect:

There may be latency issues and unstable service quality.

Packets need to be reassembled at the destination, which can cause additional delay.

For example, the Internet uses packet commutation.

3. Message Switching

Message commutation transmits data in the form of large messages from source to destination through relay points (network nodes).

Advantage:

No need to set up a fixed line.

Flexibility in routing messages through different nodes.

Defect:

Relay nodes need enough memory to store the entire message before forwarding.

Increases the likelihood of errors or loss of information if a relay node fails.

For example: Email uses message commutation.

Devices that support network commutation

Switch: Device used in a LAN to forward data packets based on MAC address. Switch operates at layer 2 (Data Link) of the OSI model.

Router: Device that forwards data packets between different networks based on IP address. Routers operate at layer 3 (Network) of the OSI model.

Hub (Signal Splitter): Simple, unintelligent device that forwards all signals to all other ports. Hub operates at layer 1 (Physical) of the OSI model.

Process for determining commutation in network design

Requirements analysis:

Determine the type of data to be transmitted (data, audio, video).

Evaluate bandwidth, latency, and reliability requirements.

Determine the number and type of devices to connect.

Choose commutation method:

Based on performance and resource requirements, choose the appropriate commutation method: circuit, packet, or message.

Link structure design:

Determine the location of switching devices (switch, router, hub).

Determine how to connect devices to optimize performance and ensure redundancy.

Configuration and deployment:

Configure the switches to ensure they operate properly.

Test and optimize network performance after deployment.

Illustration

Office network: Use a switch to connect computers in a small office, forming a LAN with a star topology. Switches forward data packets between computers based on MAC addresses.

Enterprise network: Use a router to connect LANs at different branches of a business, forming a WAN. Routers forward data packets based on IP addresses, ensuring connectivity between branches

**3. Communication speed and bandwidth requirements :**

Transmission Speed

Communication speed, or data rate, is the rate at which data is transmitted over a network. Measured in bits per second (bps), kilobits per second (kbps), megabits per second (Mbps), or gigabits per second (Gbps). This is an important index that determines the data transmission capacity of the network.

Factors affecting communication speed:

Cable type and transmission medium: For example, fiber optic cables have higher communication speeds than copper cables.

Network devices: Switches, routers, and other network devices must support high communication speeds.

Transmission distance: Communication speed may decrease as transmission distance increases, especially in wireless transmission media.

Bandwidth Requirements

Bandwidth is the maximum capacity that a network can transmit in a certain period of time, usually measured in bits per second (bps). Bandwidth requirements depend on the type of application and the number of users in the network.

Factors that determine bandwidth requirements:

Application type: High-bandwidth applications such as video streaming, conferencing, and gaming will require more bandwidth than applications such as email and web browsing.

Number of users: The more users on the network, the higher the bandwidth requirement.

Quality of Service (QoS): Some applications require low latency and stable bandwidth to ensure quality of service

**4. Discuss the operating principles of networking devices and server types :**

1. Router (Router)

Function: Connects different networks and routes data traffic between them.

How it works: Router receives data packets from a network and uses a routing table to determine the best path to deliver that data packet to the final destination.

2. Switch (Switch)

Function: Connect devices in the same LAN, helping to transfer data directly between devices.

Operating principle: Switch operates at layer 2 of the OSI model, using MAC addresses to forward data packets to the correct port connecting to the destination device.

3. Hub (Signal splitter)

Function: Connect multiple devices in one LAN and transmit signals to all ports.

Operating principle: Hub receives a signal from one port and rebroadcasts that signal to all other ports without regard to destination. Hub operates at layer 1 of the OSI model.

4. Modem (Modulator-Demodulator)

Function: Converts digital signals from the computer into analog signals for transmission over telephone lines and vice versa.

Operating principle: Modem encodes digital signals into analog signals when sending and decodes analog signals into digital signals when received.

5. Access Point (Access Point)

Function: Connect wireless devices to wired network, expand wireless network range.

Operating principle: Access Point receives wireless signals from devices and transfers that signal to the wired network via Ethernet cable.

Operating principles of different types of servers

A server is a computer system that provides resources, services and data to other computers on the network.

**5. Discuss the relationship between workstation hardware and network software**.

Performance and compatibility

Workstation hardware

1. CPU and RAM: Powerful CPU and enough RAM help to quickly handle network requests and run network applications smoothly.

Network Card (NIC - Network Interface Card): Network Card supports high speed and the latest technologies such as Gigabit Ethernet, Wi-Fi 6 to ensure fast and stable data transfer speed.

Software network

Operating system (OS): The operating system must best support the driver's latest hardware to ensure optimal performance. Operating systems such as Windows, macOS and Linux regularly update these drivers.

Application network: Applications such as web browsers, email software, and communication applications need to be compatible with the hardware to avoid lag.

2. Security

Workstation hardware

TPM (Trusted Platform Module): The TPM chip provides hardware security for operations such as disk encryption, authentication, and data protection.

Card networks have security functions: Some card networks have built-in security features such as firewalls and access control.

Software network

Antivirus software and firewalls: Security software needs to work effectively on hardware to protect workstations from cyber threats.

Update security systems: Operating systems and network software must be updated regularly to patch security drives.

3. Scalability and performance

Workstation hardware

Expand port connectivity: Workstations need to have enough connection ports to easily expand and connect to other device networks.

Supports many standard connections: Supports different standard connections such as Ethernet, Wi-Fi, Bluetooth.

Software network

Support for multiple network protocols: Network software needs to support multiple protocols such as TCP/IP, UDP, FTP, HTTP/HTTPS to be compatible with other devices and applications.

Flexible configuration capabilities: Applications and service networks need to be configurable to optimize the specific hardware required.

4. User experience and interface

Workstation hardware

High screen resolution: Provides a clear visual experience, especially important when working with web applications and media tools.

Input devices: Good quality keyboard and mouse help operate quickly and accurately when using network applications.

Software network

User-friendly interface: Network software needs to have an interface that is easy to use and optimized for workstation hardware.

Good integration with the operating system: Network applications need to integrate well with the operating system to provide a seamless experience.

5. Management and supervision capabilities

Workstation hardware

Remote management feature: Hardware that supports remote management helps network administrators easily control and configure devices remotely.

Hardware monitoring tools: Tools such as SMART for hard drives and CPU temperature monitoring help detect hardware problems early.

Software network

Network management software: Tools such as Microsoft SCCM, SolarWinds help manage and monitor system networks effectively.

Reporting and alerting features: The software provides detailed reports and timely alerts on network performance and security

**6. Explore a variety of servers and consider choosing a server for a given situation, with regard to cost and performance optimization :**

1. Dedicated Server (Dedicated Server)

Characteristics: Separate server dedicated to one customer or application.

Advantages: High performance, good security, flexible customization.

Disadvantages: High cost, requires management and maintenance skills.

2. Virtual Private Server (VPS - Virtual private server)

Characteristics: The physical server is divided into many virtual servers, each virtual server operates as a separate server.

Advantages: Lower cost than dedicated server, resources are allocated flexibly, easy to expand.

Cons: Performance may be affected by other VPS on the same physical server.

3. Cloud Server (Cloud Server)

Characteristics: Virtual servers are deployed on the cloud platform, resources can be expanded according to needs.

Advantages: Flexible scalability, only pay for resources used, high availability.

Disadvantages: Costs can increase if not managed well, depending on the service provider.

4. Shared Hosting (Shared Hosting)

Characteristics: Multiple websites share resources on the same physical server.

Advantages: Low cost, easy to use for small websites.

Cons: Low performance, less security, less customization.

5. Colocation Server (Server located in the data center)

Characteristics: Customers own the server but locate it at the service provider's data center.

Advantages: Full control of the server, high security, saving infrastructure costs.

Disadvantages: High moving and maintenance costs, requires management skills**.**

\* Situation: Personal website or blog

Requirements: Low cost, easy to manage, does not require high performance.

Suggested choice: Shared Hosting

Shared Hosting: Low cost, easy to use, suitable for small websites or personal blogs with low traffic.

\*Optimize costs and performance

When choosing a server, cost and performance optimization are important factors. Some suggestions below:

1. Assess actual needs

2. Use monitoring and optimization tools

3. Choose a suitable service provider

4. Consider contract and payment options

**7. Evaluate the topology and protocol suite chosen for a given scenario and how it represents efficient use of the network :**

Network link configuration:

1. Star configuration:

Features: The device connects directly to a central control, such as a switch or hub.

Advantages: Easy to manage, good scalability, good error setting ability.

Show results: Star configuration is suitable for networks with many connected devices and operational management requirements. Using switches instead of hubs in this architecture provides greater performance and security.

2. Mesh configuration:

Characteristics: Each device is directly connected to all other devices in the network.

Advantages: High reliability, self-healing ability, not dependent on a single point.

Show results: Mesh configurations are suitable for networks that require high reliability and auto-healing capabilities, such as in networks where loss of connectivity can cause serious problems.

3. Hybrid configuration:

Characteristics: Combines elements of different topologies such as Star, Mesh, or Ring.

Advantages: Flexible, can be optimized for network tools requirements.

The results show: Hybrid configurations are often used in large or diverse networks, where a single linking method does not meet all requirements.